

FIG.1

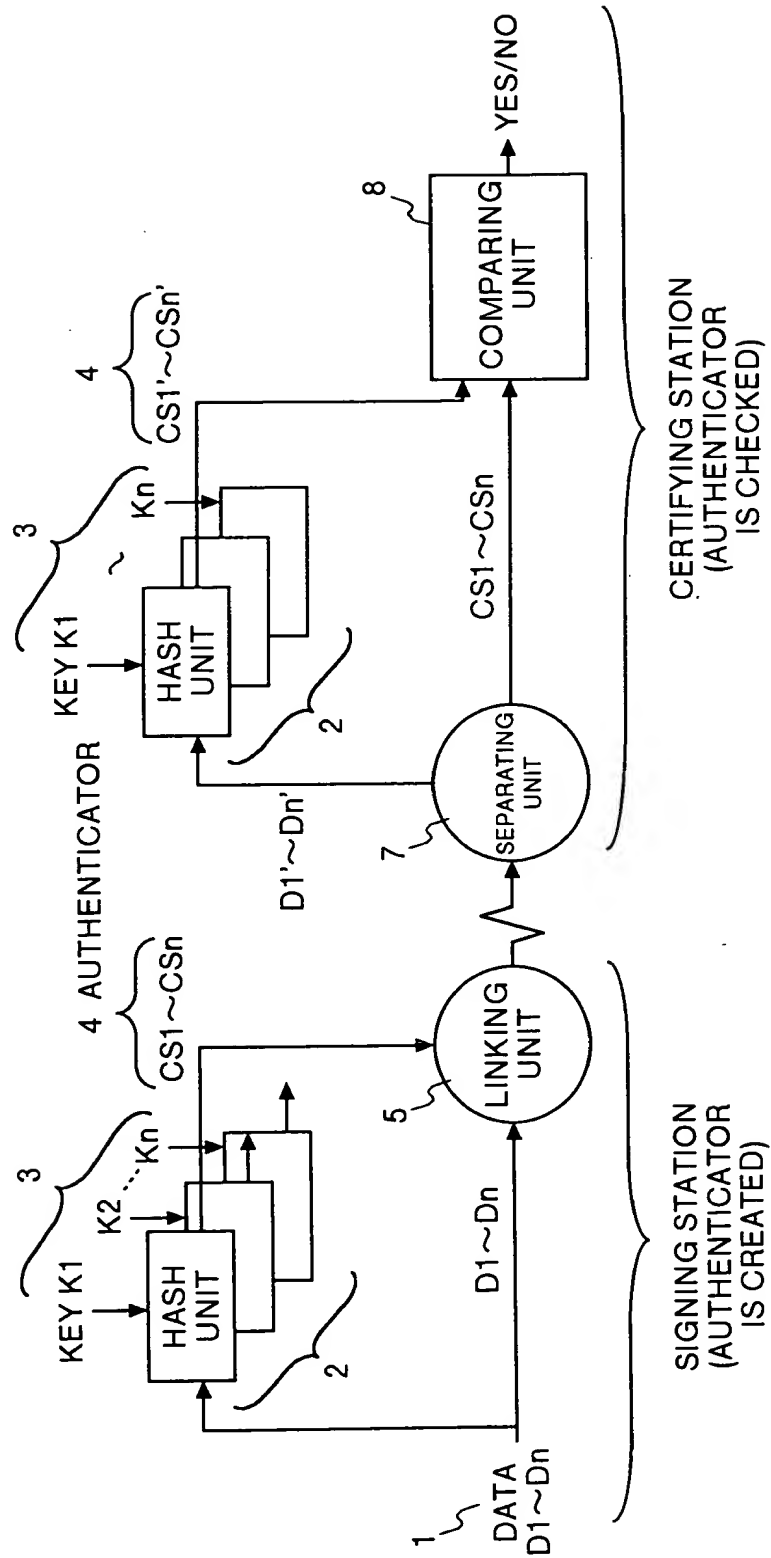


FIG.2A

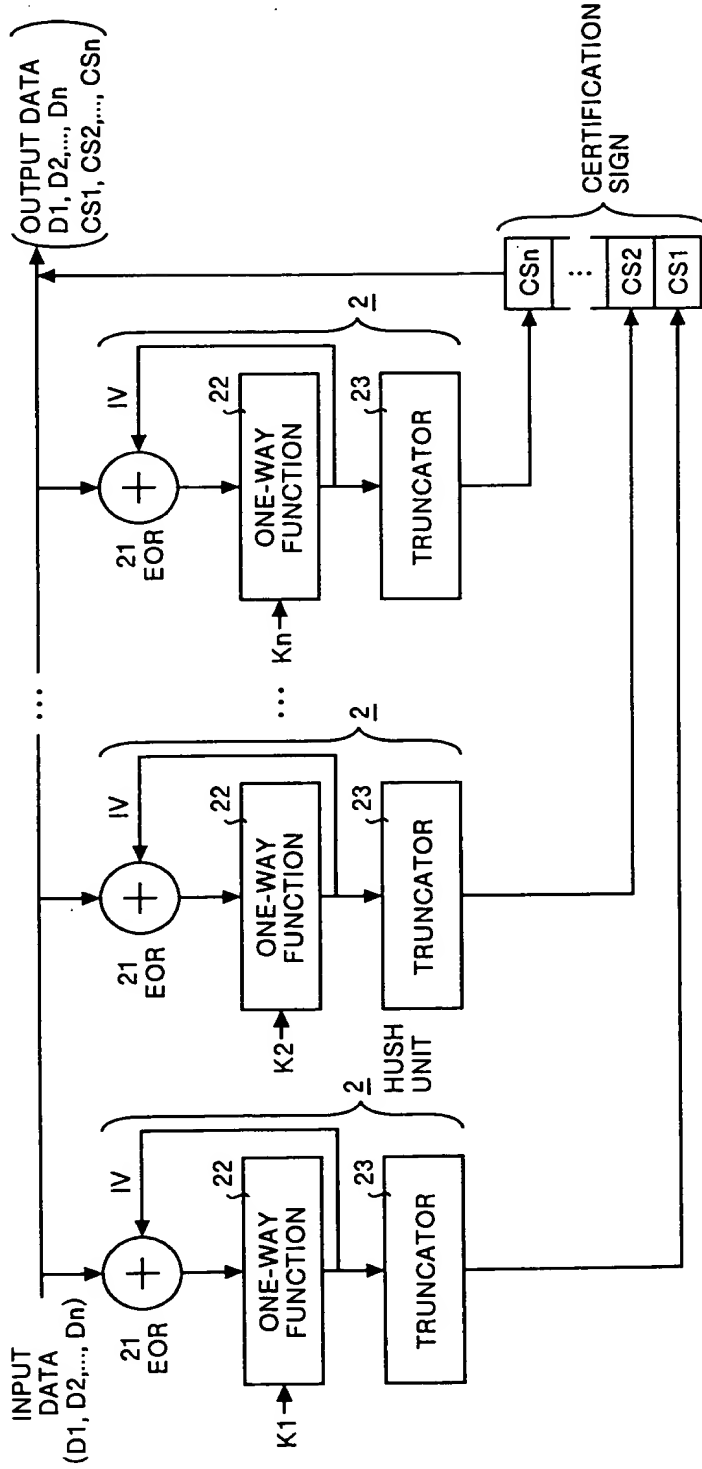


FIG.2B

- (b-1)CS1-GENERATING PROCESS
- ① → IV = PUBLIC CONSTANT
 - ② → EK1[IV(+D1)] = L11
 - ③ → EK1[L11(+D2)] = L12
 - ...
 - ④ → EK1[L1(n-1)(+Dn)] = L1n
 - ⑤ → Tr[L1n] = CS1
- (b-2)CS2-GENERATING PROCESS
- IV = PUBLIC CONSTANT
 - EK2[IV(+D1)] = L21
 - EK2[L21(+D2)] = L22
 - ...
 - EK2[L2(n-1)(+Dn)] = L2n
 - Tr[L2n] = CS2
- (b-3)CS3-GENERATING PROCESS
- IV = PUBLIC CONSTANT
 - EK3[IV(+D1)] = L31
 - EK3[L31(+D2)] = L32
 - ...
 - EK3[L3(n-1)(+Dn)] = L3n
 - Tr[L3n] = CS3

FIG. 3A

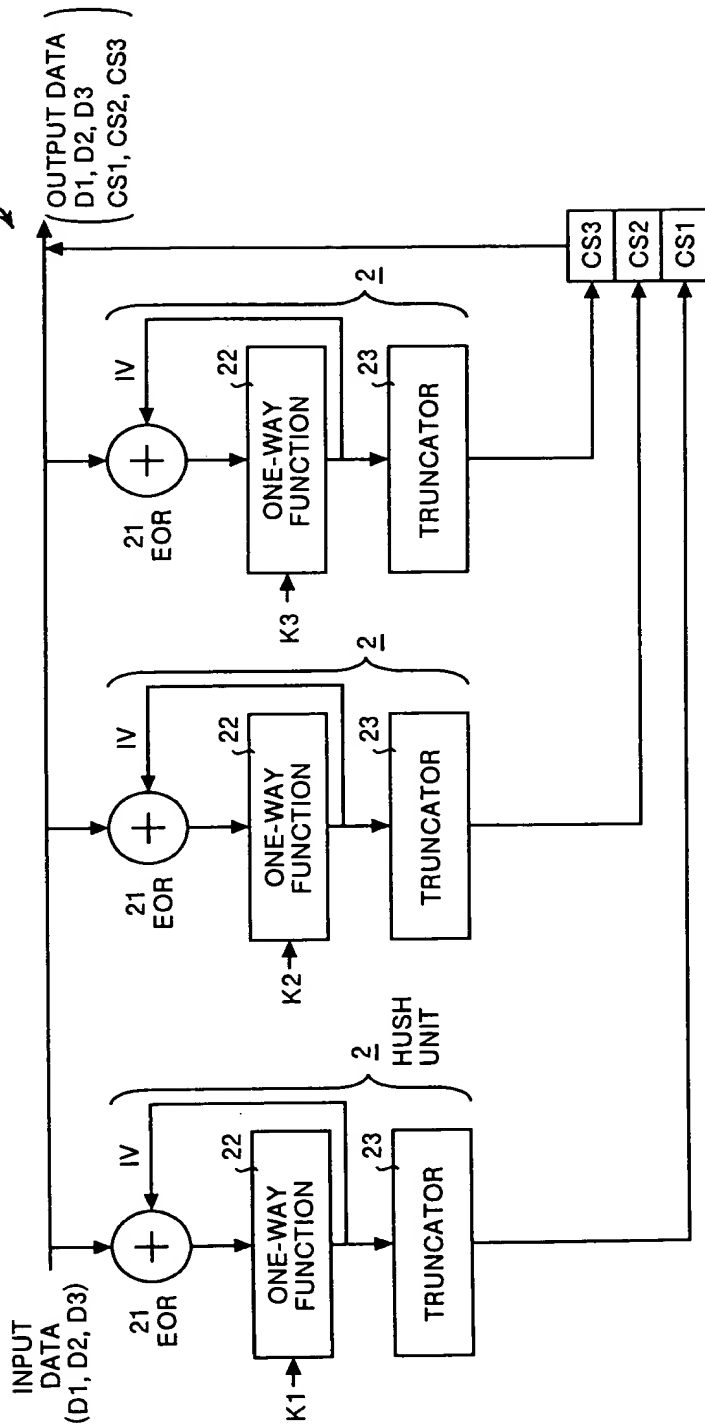


FIG. 3B

- (b-1)CS1-GENERATING PROCESS
- ① → IV = PUBLIC CONSTANT
 - ② → EK1[IV(+)D1] = L11
 - ③ → EK1[L11(+)D2] = L12
 - ④ → EK1[L12(+)D3] = L13
 - ⑤ → Tr[L13] = CS1
- (b-2)CS2-GENERATING PROCESS
- IV = PUBLIC CONSTANT
- EK2[IV(+)D1] = L21
- EK2[L21(+)D2] = L22
- EK2[L22(+)D3] = L23
- Tr[L23] = CS2
- (b-3)CS3-GENERATING PROCESS
- IV = PUBLIC CONSTANT
- EK3[IV(+)D1] = L31
- EK3[L31(+)D2] = L32
- EK3[L32(+)D3] = L33
- Tr[L33] = CS3

FIG.4A

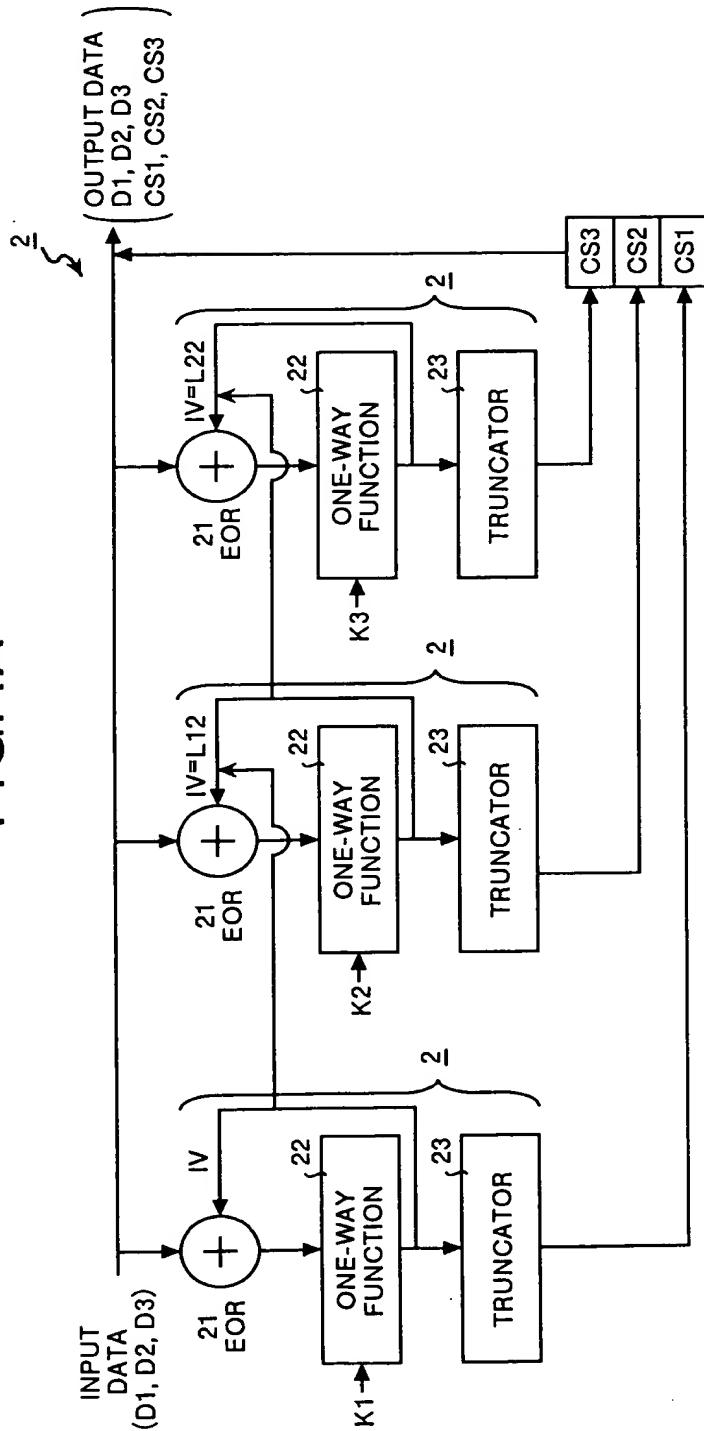
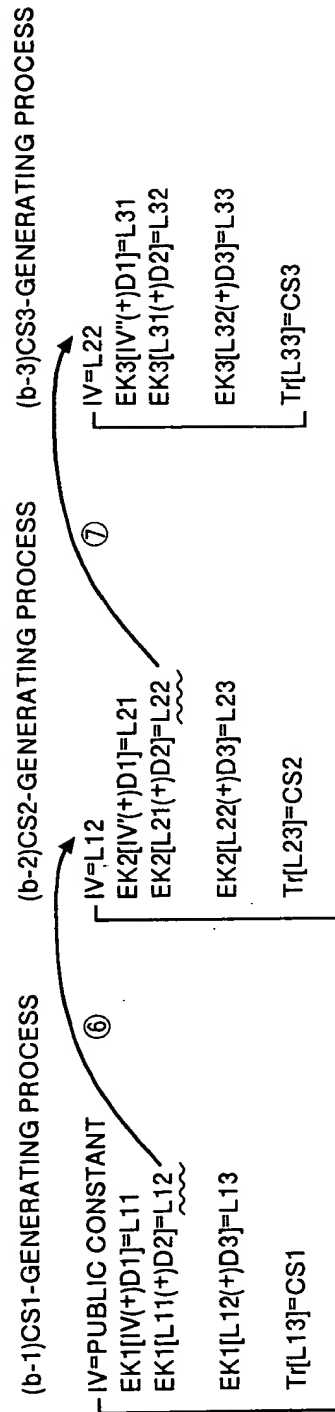


FIG.4B



[illegible]